物联网网络信息安全问题浅析

（来源：中国信通院网站，2019-04-28）

从1995年比尔•盖茨首次提及物联网概念到今天，物联网已成为新一代信息通信技术发展的典型代表，在经历了“虚张声势”的概念炒作阶段后，目前已进入到全面实践应用的新阶段，正深刻改变着传统产业形态和人类生产生活方式。然而，随着近年来物联网安全攻击事件日益频发，对用户隐私、基础网络环境的安全冲击影响也越来越突出。本文从物联网当前面临的安全形势、物联网存在的安全风险、产生安全问题的主要因素分析入手，进而提出相关促进物联网健康有序发展的对策建议。

一、万物互联下网络信息安全问题备受关注

（一）各类垂直应用领域受到物联网安全问题影响

物联网应用涉及国民经济和人类社会生活的方方面面，然而近年来多领域发生安全事件：在智慧城市领域，2014 年西班牙三大主要供电服务商超过30%的智能电表被检测发现存在严重安全漏洞，入侵者可利用该漏洞进行电费欺诈，甚至关闭电路系统。在医疗健康领域，早在2007年时任美国副总统迪克•切尼心脏病发作，调查部门怀疑缘于他的心脏除颤器无线连接功能遭暗杀者利用，这被视为物联网攻击造成人身伤害的可能案例之一。在工业物联网领域，安全攻击事件则危害更大，2018 年台积电生产基地被攻击事件、2017 年的勒索病毒事件、2015 年的乌克兰大规模停电事件都使目标工业联网设备与系统遭受重创。

（二） 物联网安全问题给隐私保护带来严重威胁

随着物联网的应用，涉及用户隐私的海量数据将被各类物联网设备记录，其数据安全隐患也愈加严重。2015 至今国内外发生多起智能玩具、智能手表等漏洞攻击事件，超百万家庭和儿童信息、对话录音信息、行动轨迹信息等被泄露；2017 年 7 月美国某公司自动售货机遭黑客攻击，被窃取了数十万用户信用卡账户以及生物特征识别数据等个人信息；我国某安防公司制造的物联网摄像头被爆出多个漏洞，黑客可使用默认凭证登录设备访问摄像头的实时画面。此外，据有关数据显示，10000 户家庭每天大约能够生成多达 1.5 亿个离散数据点。据 IDC 报告显示，2020 年全球物联网设备将有 200-250 亿台。海量用户隐私数据被庞大的物联网设备所承载记录，其安全风险系数也被极具放大。

（三）各组织机构纷纷关注物联网安全

近两年举办的 RSA 大会、Black Hat 等安全大会都对物联网安全高度关注，CES 等会议也加大对物联网安全的关注。在 RSA 2018 安全大会上，诸多关于物联网安全漏洞的讨论被提及，特别是物联网终端设备或智能家居产品。2016 年 8 月，在一年一度 Black Hat 大会上，物联网安全成为十大值得关注的安全威胁之一，会上黑客展示了对联网汽车、智能灯泡、ATM 等物联网设备的攻击。在 CES 2016 大会上，物联网安全的关注度被排在了智能家居、可穿戴设备和无人驾驶汽车之前，位居第一位。

二、物联网网络的安全风险分析

当前，物联网逐渐形成了以“云、管、端”为主的三层基础网络架构，与传统互联网相比较，物联网的安全问题更加复杂。

（一）“端”——终端层安全防护能力差异化较大

终端设备在物联网中主要负责感知外界信息，包括采集、捕获数据或识别物体等。其种类繁多，包括 RFID 芯片、读写扫描器、温度压力传感器、网络摄像头、智能可穿戴设备、无人机、智能空调冰箱、智能汽车……体积从小到大，功能从简单到丰富，状态或联网或断开，且都处于白盒攻击环境中。由于应用场景简单，许多终端的存储、计算能力有限，在其上部署安全软件或者高复杂度的加解密算法会增加运行负担，甚至可能导致无法正常运行。而移动化作为物联网终端的另一大特点，更是使得传统网络边界“消失”，依托于网络边界的安全产品无法正常发挥作用。加之许多物联网设备都部署在无人监控场景中，攻击者更容易对其实施攻击。

（二）“管”——网络层结构复杂通信协议安全性差

物联网网络采用多种异构网络，通信传输模型相比互联网更为复杂，算法破解、协议破解、中间人攻击等诸多攻击方式以及 Key、协议、核心算法、证书等暴力破解情况时有发生。物联网数据传输管道自身与传输流量内容安全问题也不容忽视。目前已经有黑客通过分析、破解智能平衡车、无人机等物联网设备的通信传输协议，实现对物联网终端的入侵、劫持。在一些特殊物联网环境里，传输的信息数据仅采用简单加密甚至明文传输，黑客通过破解通信传输协议，即可读取传输的数据，并进行篡改、屏蔽等操作。

（三）“云”——平台层安全风险危及整个网络生态

物联网应用通常是将智能设备通过网络连接到云端，然后借助 App 与云端进行信息交互，从而实现对设备的远程管理。云平台能够对物联网终端所收集的数据信息进行分析与管理，以及对网络的安全

管理，如对设备终端的认证，对攻击的应急响应和监测预警，以及对数据信息的保护和安全利用等。物联网平台未来多承载在云端，目前云安全技术水平已经日趋成熟，而更多的安全威胁往往来自内部管理或外部渗透。如果企业内部管理机制不完善、系统安全防护不配套，那一个小小的逻辑漏洞就可能让平台或整个生态彻底沦陷。而外部利用社会工程学的非传统网络攻击始终存在，一旦系统成为目标，那么再完善的防护措施都有可能由外至内功亏一篑。

三、影响物联网行业安全的主要因素

多方面的因素导致了物联网已经逐步成为网络信息安全“重灾区”，其中既有物联网技术本身技术特点逐步累积形成的特性，也有新兴行业在高速发展过程中存在的通病。

一是产业结构复杂。物联网在发展过程中逐渐形成了较为完整的生态体系，但在三层架构的基础上更涉及了众多产业链环节，导致参与角色众多、结构复杂。从终端层的硬件芯片、传感器、无线模组，到网络层各通信运营商，再到平台应用层的软件开发、系统集成、平台服务，这其中各个环节都在整个产业链中不可或缺。这就需要各个环节紧密配合、统一认识才能确保不出现大的安全问题。

二是安全意识淡薄。据 Gartner 发布的数据显示，到 2020 年，全球物联网市场规模将达 1.9 万亿美元。而在产业高速发展、规模急剧扩张的背后，是物联网厂商安全意识淡薄，安全投入不足的现状。一方面，物联网设备数量庞大、价格低廉，很多厂商为压缩成本则对安全投入严重不足。Gartner 预测 2018 年全球物联网安全支出将达到 15 亿美元，年增长率保持在 27%左右，这跟市场规模相比甚至不足 1‰，差距较大。另一方面，多数物联网设备和硬件制造商无法像

互联网企业一样重视安全，缺乏安全意识和人才储备。AT&T 对全球5000 多家企业调查发现，85%的企业正在或打算部署物联网设备，而仅 10%企业表示有信心保护设备免受黑客攻击。

三是监管政策及标准体系匮乏。2013 年国务院在《关于推进物联网有序健康发展的指导意见》中提出“要加强物联网重大系统和应用的安全测评、风险评估和安全防护工作，保障物联网重大基础设施、重要业务系统和重点领域应用的安全可控”，但目前尚未进入实质性阶段，相关政策法规有待落地。在安全标准体系建设方面，虽然行业内已有多个物联网组织在推进物联网标准体系建设，但由于物联网技术更新快、应用场景丰富，导致物联网标准体系建设步伐滞后于物联网发展，且缺乏完善的安全标准体系和成熟的安全解决方案。

四、关于进一步加强物联网网络信息安全的对策建议

物联网发展已经进入快车道，规模化应用部署也在提速，物联网安全若没有配套措施手段将无法跟上其发展步伐。建议我国在物联网安全政策、标准、应用和人员培训等方面进一步推进，加大安全监管力度，引导和促进整个产业对于安全问题的关注，提高从业人员和用户对于安全风险的重视，保障物联网产业持续健康发展。

在监管层面，加强监管落实，推动物联网领域的安全标准制订。建议加强整体行业安全管理，建立安全性合规性检测机制，提高行业准入门槛，约束发展乱象，从安全框架体系、安全测评、风险评估、安全防范、安全处置方案等方面推动标准规范制订和落地。

在产业层面，推动构建物联网全生命周期立体防御体系。在硬件、操作系统、通信技术、云端服务器、数据库等各个模块之间做好统一的安全体系建设，从开发到制造、集成，把安全设计融入到物联网产

品生命周期每个步骤，从芯片到硬件、软件、系统，将安全防护作为物联网每个环节必要的配套手段，推动整个产业对安全需求从被动转为主动，让安全紧跟产业发展步伐。

在技术层面，加快物联网安全技术发展及防范技术研究。建议设备厂商、研究机构等加大对物联网软硬件、操作系统、通信协议、云平台等方面的安全技术的关注力度，研发有效的安全威胁监测发现技术和安全防护技术，团结行业力量打造物联网安全生态。

在宣传层面，普及信息安全知识，提高安全意识。建议企业树立正确的发展观念，同步重视网络信息安全，同时对物联网从业人员进行安全知识普及和技术培训，提高从业人员的安全意识和知识技能。此外，建议提高用户网络信息安全意识，在挑选使用物联网产品的同时注重安全防范。（作者：张昊星、柳青）

原文链接：http://www.caict.ac.cn/kxyj/caictgd/tnull_196523.htm，转载请注明。